A New Approach for Video Encryption Based on Modified AES Algorithm

Asst. Prof: Dr. Salim Ali Abaas¹, Ahmed Kareem Shibeeb²
Dept. of Computer Science, College of Education, Al-Mustansiriya University, Baghdad, Iraq

Abstract: The security of video applications such as commercial videos, military videos and others have become an important field of research recently. One of the most secure algorithms is Advanced Encryption Standard (AES) algorithm; however, this algorithm is inefficient for dealing with video encryption due to its slowness property. This paper proposes a new modified AES to make it more suitable for encrypting digital video. The modification focuses on the slowest transformation in original AES which is mix column transformation and replace them with new Henon map chaotic based mask and one mix columns transformation. Resulting in a significant reduction in encryption and decryption time and enhance the security level of AES algorithm, and also the key space is increased as observed in the simulation results of proposed system.

Keywords: AES-128, Chaotic mask, Henon map, Sub-Byte, Mix columns.

I. Introduction

1.1 Background

With the rapid progress of Digital Communication Technology, the security of digital image/video plays a significant role in computing technology. Recently, the main consideration in data storage and transmission is the information security [1]. An increasing amount and security sensitivity of the information, such as audio, images, video and other multimedia applications make it requires quick and safe ways to achieve its security [2]. There are many approaches for the information security which include steganography and cryptology. The block ciphers have played a vital role in the science of cryptography when the Data Encryption Standard algorithm (DES) has been introduced. The small block size and short key problem of the DES algorithm makes it more vulnerable to Differential Cryptanalysis (DC) and Linear Cryptanalysis (LC), in addition to security problems, the DES algorithm is slow encryption algorithm. The Advanced Encryption Standard algorithm (AES) is new encryption standard instead of the DES algorithm according to the viewpoint of National Institute of Standards and Technology (NIST). The advanced encryption standard algorithm provides multiple keys lengths (128 bits, 192 bits, and 256 bits) on the contrary of the data encryption algorithm which provides short key length (56 bits), as well as the AES very powerful against all known attacks and faster than DES algorithm. Although the accepted speed of AES algorithm, but it is not efficient to encrypt digital video due to the large size of the video compared to other multimedia applications [3]. So, this paper proposes an appropriate modification for original AES-128 to make it more suitable for digital video encryption. Modification will focus on the mix columns step to modify it with new chaos based matrix to reduce the time of encryption and decryption processes, and at the same time provide high diffusion and confusion in the proposed algorithm.

1.2 Literature Review

Several attempts have been made in the literature toward AES algorithm enhancement and multimedia encryption. Hephzibah and Gnanou [4] introduce a chaos-based video encryption based on the Lorenz system, when the plain video was divided into frames, then checked whether the frame was a large size, it will get macro-blocks from the frame for encrypting. And take advantage of the Lorenz system properties for the purpose of frame pixels confusion. As observed in [4], the proposed system is fast and insecure.

S. Kamali et al. [5] introduce a new modified AES algorithm that decreased the pattern appearance and to encrypt square image only by adjusting the shift rows step based on the first cell value of the state array, if its value is odd, then the first and third rows are remaining in an original state, whereas the second and fourth rows are shifted one and three bytes to the left, respectively. Meanwhile, if its value is even, then the first and fourth rows are unchanged, while the second and third rows are shifted three and two bytes to the right, respectively. Likewise, the proposed method in [6], it uses the same of previous method to reduce the calculation of the video encryption completely. This modification is a quick somewhat, but not enough for encrypting video. In [7], divide the plain image into blocks then reordering of the block’s pixels is performed by changing the positions of pixels. Finally, these blocks are passed randomly to AES algorithm. This method used to decrease the correlation between plain image and cipher image and disregards the increase in encryption time. However, three modifications on AES algorithm is proposed by S. Wadi and N. Zaina to make it more suitable for encrypting HD images by increasing AES security and reducing its computation cost and hardware.
requirement through, using the mix columns transformation as additional transformation in key schedule operation to enhance the security level, reducing the mix columns step in AES-128 bits to five instead of ten to reduce the encryption time and constructing simple and one S-box for encryption and decryption processes to reduce the requirement of hardware. The first modification increases the security level and requires more time for the encryption process. On the contrary, the second modification which provides less encryption time and low security level than original AES, while the third modification reduces the security level of AES as a result of the low nonlinearity of new S-box as obtained in [8].

II. Advanced Encryption Standard Algorithm Specification

The AES is designed to agree with principles of Substitution-Permutation Network mechanism. Thus it involves some of operations during the encryption and decryption; these operations take 4×4 matrix called the state which represents 16 byte of data as input. There are four basic operations used over the encryption process to encrypt the plain text which are: Substitution byte by using the Substitution Box (S-box), Shifting Rows, Mixing Columns and XOR’ing with Round Key. However, at the decryption process the inverse of previous steps will be used to decrypt original data which are: InvSubBytes, InvShiftRows and InvMix-Columns in addition to AddRoundKey transformation. The sub-keys for number of rounds (Nr) that are used in encryption and decryption processes will be created by using an operation of the key schedule [9].

2.1. Stages of Rounds
2.1.1 Sub-Byte / Inverse Sub-Byte

The Sub-Byte function uses a substitution table (S-box) to substitute the bytes of state array. The byte substitution step used to increase the security level of AES algorithm because it agrees with nonlinearity requirement [10]. However, in the decryption process the InvS-box table instead of S-box will be used to implement Inverse Sub-Byte operation.

2.1.2 Shift Rows/ Inverse Shift Rows

Some references assume the shift rows operation as the second operation at the encryption round; while it can be applied before the Sub-Byte step without any effect on the algorithm. In shift rows operation the data matrix processes in row-by-row fashion. The first row remains unchanged, while the rows numbered with 2, 3 and 4 of the state matrix are rotated one, two and three bytes in cyclic way to the left-side, sequentially. In another side, the inverse shift rows operation is obtained by remaining the first row unchanged and rotating the rows numbered with 1, 2, and 3 cyclically rotate to the right-side, with one, two and three bytes, respectively [11].

2.1.3 Mix Columns / Inverse Mix Columns

After applying the Shift Rows operation, the Mix Columns step is performed, in this step each column in the state array is multiplied by a known 4×4 matrix defined as follows:

\[
\begin{bmatrix}
02 & 03 & 01 & 01 \\
01 & 02 & 03 & 01 \\
01 & 01 & 02 & 03 \\
03 & 01 & 01 & 02 \\
\end{bmatrix}
\]

The multiplication operation is implemented on this matrix is not a normal multiplication. Rather, the multiplication operation is carried over a Galois-Field (GF), where the multiplication operation can be obtained as follows: Multiplication by 01 means no change, multiplication by 02 means is handled as shifting byte to the left with one bit, and multiplication by 03 treated as shifting to the left, then XOR’ing with the operand [12]. The Inverse of Mix Column operation is applied by multiplying each column of a state array by another special matrix defined as follows:

\[
\begin{bmatrix}
0E & 0B & 0D & 09 \\
09 & 0E & 0B & 0D \\
0D & 09 & 0E & 0B \\
0B & 0D & 09 & 0E \\
\end{bmatrix}
\]
2.1.4 AddRoundKey / Inverse AddRoundKey

The first AddRoundKey operation is implemented with the master key before starting the regular rounds operations of the algorithm. The AddRoundKey transformation is the part of the algorithm which takes each byte in the state array and XOR this byte with a corresponding byte in the round key.

2.2 Key Expansion (Key Schedule)

The key expansion or the key schedule is an operation of generating a number of sub-keys from the initial key for each round to be used in the AddRoundKey operation. Therefore, the number of needed sub-keys is equal to the number of rounds (Nr) and hence the round keys contain 44 words (where each word equal to four bytes) will be generated for AES-128. When the words indexed from 0 to 43, the first four words (W0, W1, W2, W3) are filled with the given cipher key, however columns in locations that are a multiple of 4 (W4, W8, W12 … etc.) will be computed by three operations which are: The RotWord, The SubWord and add the result of a RotWord and SubWord operations with word Wi-4 and with a Round Constant (Rcon[i]) [13].

III. Chaotic HENON Map

The noticeable properties of chaotic systems which are sensitivity to the initial condition and control parameter values, unpredictability and their capability of generating random numbers made them used over the last years in many cryptography [13]. There are many chaotic maps with multi dimension, one of these chaotic maps is Henon map that is a two dimension discrete-time nonlinear map explained by:

\[
\begin{align*}
Y_{n+1} &= 1 - aY_n^2 + Z_n \\
Z_{n+1} &= bZ_n
\end{align*}
\]

in each of the equation, the current and next chaotic states are \((Y_n,Z_n)\) and \((Y_{n+1},Z_{n+1})\) respectively, while the values of \(a\) and \(b\) are map parameters. Any of the previous parameters \((a, b)\) or initial states \((Y_0,Z_0)\) could be to become a key to the aforementioned map [14,15]. The Henon map exhibits chaotic behavior when \(a \in [1.16,1.41]\) and \(b \in [0.2,0.3]\). The parameters values that commonly used in Henon system are \((a= 1.4, b = 0.3)\) as shown in Figure (1).

**Figure (1):** The strange attractor of Henon map with control parameters values \((a= 1.4, b = 0.3)\).

IV. The Proposed Scheme

The multiplication over Galois Field is one of the greatest importance mathematical operation applied during the mix column step and one of the high calculation and computational overhead operation in AES [16]. Therefore, the mix columns and its inverse are two of the slower operations in the encryption and decryption process. This is due to the fact that, it involves matrices multiplication over Galois Field. This problem is opposed to adapt the original AES to encrypt video. To overcome the problem one mix columns for first round will be performed in addition to new chaotic mask instead of remained mix columns steps and their inverse in AES-128 for encrypting video frames due to the superiority of proposed scheme in terms of speed and the sensitivity to initial conditions and control parameters and also the increase of key space and key sensitivity. This modification is as shown in the following encryption and decryption algorithms:
A New Approach For Video Encryption Based on Modified AES Algorithm

**Encryption Algorithm:**
- The initial value \((Y_0, Z_0)\) and two control parameters \((a, b)\) of Henon map in addition to the cipher key that expanded into array of 176 bytes as initial key of the algorithm.
- Due to the high sensitivity of the last three numbers for each output sequence, the proposed system takes the remainder of dividing the last three number of the map equations output \((Y,Z)\) on the 256 to convert them into hexadecimal values, and save it in 4x4 matrix as chaotic mask.
- Sort the matrix values in ascending order.
- Assign the new index of sorted matrix as permutation key and matrix values as substitution key.
- Read the plain video and extract its frames. Then each frame is divided into blocks of the size 128 bits that is placed into the state array.
- Add the state array with cipher key.
- Substitute each byte with Sub-Byte transformation.
- Apply shift rows transformation.
- Use one mix columns transformation for first round and replace the remained mix columns transformations (from the second round to \(N_r - 1\)th round) with new chaotic mask for scrambling the bytes positions of the state array by using permutation key, then the scrambled state array is XORed with chaotic mask values (substitution key).
- XOR the current state array with round key.
- Reassembling the encrypted frame from the encrypted state array, then collecting the cipher frames to create a cipher video.

**Decryption Algorithm:**
- Set the Henon map keys and cipher key which will also expand.
- Construct the Henon map based chaotic mask.
- Sort the chaotic mask values.
- Assign the substitution and permutation keys based on the values of generated mask and index of sorted chaotic mask, respectively.
- Read the encrypted video.
- Apply add round key transformation.
- Perform inverse of shift rows transformation.
- Use InvS-box to apply inverse Sub-Byte transformation.
- Reapply add round key transformation.
- Perform inverse of chaotic mask stage for the first eight rounds by XOR’ing the state array with chaotic mask values, then descrambling by using the permutation key, however the ninth round will be involved mix columns transformation.
- Finally, re-collecting the encrypted frames for cipher video compositing, then save it.

The block diagram of the proposed scheme for encryption and decryption processes is shown Figure (2).

**Figure (2):** Block diagram of the proposed scheme for the encryption and decryption processes.
V. Simulation Results

5.1 Security Analysis

5.1.1 Key Space Analysis

The total number of various keys that can be used in a proposed method is also known as the key space. A high secure encryption system depends on the strength of encryption keys. Whereas the key strength is mainly dependent on the key space. In another words, the relationship between the encryption key and the cipher message should be as complex as possible so any change of one bit of the encryption key will produce a total different cipher message. To achieve high resistance against many attacks such as brute-force attack, the key space of cryptosystem must be large as possible [17]. The proposed method consists of the exist cipher key which is 2^{128} in addition to four real values that provided by the initial conditions (Y_{0}, Z_{0}) and control parameters (a, b) of Henon map, whilst each real value is 64 bits. Hence the total key space of proposed scheme is 2^{384}, which can make the brute force attack is impossible on this proposed algorithm.

5.1.2 Key Sensitivity Test

The key sensitivity for each cryptosystem means that the encrypted video must be completely different from the original video, if there is any change between encryption and decryption keys. A strong ciphering system requires large key sensitivity as much as possible to ensure security of the system. The proposed scheme is high sensitive to any small change in one of all the keys. If the keys of the proposed system are Y_{0}=0.50000001, Z_{0}=0.20000001, a=1.39999,b=0.200012 and a cipher key=abcd12349876efah, the key sensitivity test of the proposed algorithm has been applied on Rhinos(45) frame by using the same key that is used in decryption except that the value of (Y_{0}) is slightly changed to 0.50000002 and the plain frame is displayed in Figure (3).

![Figure (3): Result of key sensitivity analysis: a. Frame decrypted with incorrect key b. Frame decrypted with right key](image)

5.1.3 Resistance to Differential Cryptanalysis

The differential cryptanalysis is one of the most powerful cryptanalysis against block cipher, the differential cryptanalysis attempts to observe differences of the cipher frame in the tiny change of the original frame to find the relationship between the original frame and the cipher frame. To evaluate the cryptosystem resistance against differential attack, two measures (NPCR) and (UACI) commonly used, whereas the (NPCR) means the change rate of the number of pixels of the encrypted frame when only one pixel of the original frame is changed and the (UACI) means the unified average changing intensity which gauges the average intensity of variations between the original frame and encrypted frame [19]. Their definitions are as follows:

\[
NPCR = \sum_{i,j}^{N,M} \frac{\text{Diff}(i, j)}{M \times N} \times 100\%
\]  

\[
UACI = \frac{1}{M \times N} \left[ \sum_{i,j}^{N,M} \frac{C_1(i,j) - C_2(i,j)}{255} \right] \times 100\%
\]

In equation (2), the Diff(i, j) is determined by the initial cipher frame C_{1}(i, j) and ciphered frame that is changed some grey level of the pixels C_{2}(i, j), if C_{1}(i, j) = C_{2}(i, j) then Diff(i, j) = 0, otherwise, Diff(i, j) = 1. While M and N in both equations (2) and (3) are the width and height of the frame. The ideal NPCR and UACI values for 8-bit gray scale frames are 99.609% and 33.464%, respectively.
Table 1 shows the test results of NPCR and UACI measures for the proposed scheme that compared with original AES algorithm. It is discovered that the NPCR and UACI values of the proposed scheme are close to their ideal values. Thus, the proposed method has great capacity of resistance to the plain text attacks and differential attacks.

<table>
<thead>
<tr>
<th>Frames</th>
<th>NPCR for original AES (in %)</th>
<th>UACI for original AES (in %)</th>
<th>NPCR for Modified AES (in %)</th>
<th>UACI for Modified AES (in %)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rhinos (41)</td>
<td>99.6367</td>
<td>33.5693</td>
<td>99.6615</td>
<td>33.5298</td>
</tr>
<tr>
<td>Vipmosaicking(28)</td>
<td>99.6054</td>
<td>33.3138</td>
<td>99.6576</td>
<td>33.51</td>
</tr>
<tr>
<td>Shacky-Cart (86)</td>
<td>99.5989</td>
<td>33.4324</td>
<td>99.6223</td>
<td>33.4046</td>
</tr>
<tr>
<td>Viplane(4)</td>
<td>99.58</td>
<td>33.3485</td>
<td>99.6544</td>
<td>33.4134</td>
</tr>
</tbody>
</table>

Table (1): Measurements of NPCR and UACI for different frames.

5.2 Statistical Analysis

5.2.1 Frame Statistic Characteristic

The pixel values distribution of each frame can be reflected by Image histogram. A flat histogram of cipher frame may mean that frames resist statistic attacks [20]. Figure (4) shows the red, green and blue channel histograms of the original frame and the cipher frame. We can see that, the histogram of the cipher frame is fairly uniform distribution. Hence the proposed method does not present any clue to employ any statistical attack on the encrypted frame.

![a. Original frame](image1)

![b. Encrypted frame](image2)

![c. Histogram of original frame](image3)

![d. Histogram of encrypted frame](image4)

**Figure (4): Histogram of original frame and encrypted frame**

5.2.2 Information Entropy Analysis

Frame information entropy is defined to measure the degree of randomness or disorder in the system to give a description of the frame texture [11, 15]. Whenever the histogram analysis only shows the cipher frame in a qualitative way, the information entropy used to get the quantitative analysis. The formula for calculation entropy $H(x)$ For a frame with $n$ gray level is:

$$H(x) = - \sum_{i=1}^{n} p(x_i) \log_2 p(x_i)$$

Where $H(x)$ represents of the frame and $P(x_i)$ is the emergence probability of $x_i$. If every symbol has an equal probability, i.e. $\{x_0, x_1, x_2, \ldots x_{2^8-1}\}$ and $P(x_i) = 1/2^8 (i=0,1,\ldots,255)$, then the entropy is $H(x) = 8$ which corresponds to an ideal entropy of a 256 gray-scale image.
The entropy analysis of encrypted frame is very closed to the ideal value as obtained in Table (2). Therefore, the proposed scheme resist the entropy attacks.

![Table (2): Entropy analysis of different plain and cipher frames.](image)

### 5.3 Time Analysis

The efficiency of proposed scheme have been measured with important metric to compare among cryptosystems is to compute the encryption and decryption time [21]. Time analysis has been implemented under C#.net on a 2.20 GHz Intel® Core™ i3 CPU and 2 GB RAM - HP 650 laptop. Compared to original AES, we can show that the running speed of the proposed method is fast, when executed in the same conditions and environment, as obtained in Table (3).

![Table (3): examines quantitatively the encryption and decryption time of the original AES and proposed scheme.](image)

### VI. Conclusion

Generally, speed and secure cryptosystems are very desirable for multimedia applications. In this paper, an efficient method has been introduced for video encryption based on the combination of 2D Henon chaotic map and AES algorithm. Whereas Henon map is used to construct new chaotic mask to replace mix columns transformations except the first mix columns due to the slowness and security of the mix columns transformation in original AES. Efficiency of the method has been confirmed through above simulation results.

According to these results the proposed scheme provides high key space, high key sensitivity and less time for encryption and decryption processes than original AES as well as it offers high resistance against differential and statistical attacks.

### References


DOI: 10.9790/0661-17364451 www.iosrjournals.org 50 | Page
A New Approach For Video Encryption Based on Modified AES Algorithm


[19]. J. Zhang,”An Image Encryption Scheme Based on Cat Map and Hyperchaotic Lorenz System”, IEEE International Conference on Computational Intelligence and Communication Technology, IEEE, 2015.


DOI: 10.9790/0661-17364451
www.iosrjournals.org